REMARKS

In response to the action of December 12, 2007, applicants asks that all claims be allowed in view of the amendments to the claims and the following remarks.

Claims 1, 26, 51 and 54-85 are currently pending, of which claims 1, 26, 51 and 83-85 are independent. Claims 1, 26, 51 and 83-85 have been amended. Support for these amendments may be found in the application at, for example, page 2, line 26 to page 3, line 3; page 3, line 25 to page 4, line 5; and FIG. 1. No new matter has been introduced.

Claims 1, 36, 51, and 54-83 have been rejected under §112, first paragraph as failing to comply with the written description requirement. Applicant has amended independent claims 1, 36, 51, and 83-85 to, *inter alia*, address these issues noted in the rejection by removing the objected-to language. Applicant submits that claims 1, 26, 51 and 54-85, as currently presented, are fully compliant with § 112, first paragraph, and thus requests withdrawal of the rejection.

The specification has been objected to as failing to provide antecedent basis for the claimed subject matter. As noted above, independent claims 1, 36, 51, and 83-85 have been amended to address this issue. Applicant submits that the specification provides proper antecedent basis for the currently claimed subject matter, and thus requests withdrawal of the objection.

Claims 84 and 85 have been rejected as being unpatentable over U.S. Patent No. 6,219,793 (Li). Applicant requests reconsideration and withdrawal of this rejection because Li does not describe or suggest checking the read biological information with the stored biological information is carried out by using only the portable communication device, as recited by claims 84 and 85.

Independent claims 84 and 85 recite a method (claim 85) or a system (claim 84) for identifying an individual to identify a client. Claims 84 and 85 each recite storing the biological information of the client, reading the biological information of the client, checking the read biological information with the stored biological information, and transmitting information to the server that the checking has matched. Claims 84 and 85 also each recite that after transmitting information that the checking has matched to the server, a personal identification number

information is sent to the server and in a case that the personal identification number matches with a number stored at the server, the stored biological information can be rewritten. Claims 84 and 85 each recite checking the read biological information with the stored biological information is carried out by using only the portable communication device.

In contrast, Li's mobile telephone 102 communicates with the central authentication system (CAS) 106 to receive the fingerprint-based token for comparison with the generated token as part of the identification process. More particularly, Li discloses using a fingerprint capturing device ("FCPD") 101 to identify an individual using a portable communication device, where the fingerprint capturing device preferably is incorporated within a mobile telephone 102. See Li at col. 6, lines 54-66. The fingerprint capturing device captures a user's fingerprint information and generates a token based on the captured fingerprint information. See Li at col. 7, lines 40-46. Notably, Li's fingerprint capturing device also receives a fingerprint-based token from a central authentication system (CAS) 106 for comparison with the generated token as part of the identification process. See Li at col. 7, lines 52-55.

Li presents a flowchart in FIGS. 3A-3B that shows information being exchanged between the wireless telephone 102 and the central authentication system (CAS) 106 over the PSTN or Internet 105 as part of the identification process. More particularly, Li's flowchart in FIGS. 3A-3B begins with a user dialing a telephone number using the wireless telephone 102 (step 300) and sends information to the central authentication system (CAS) 106 from the mobile switching center (MSC) 103 using the PSTN or Internet 105 (step 304). See Li at FIG. 3A and col. 10, lines 33-35 and lines 44-46. The CAS 106 sends to the wireless telephone 102 a token CK 202 associated with the MIN of the wireless telephone 102. See Li at FIG. 3A (step 307) and col. 10, lines 47-54. The fingerprint capturing device (FCPD) 101 (which is preferably incorporated into the wireless telephone, see Li at col. 6, lines 54-66) requires the user to input the user's fingerprint locally, so that a token can be generated from the captured fingerprint information. See Li at FIG. 3A (step 308) and col. 10, lines 57-58. Importantly, the fingerprint capturing device (FCPD) 101 compares the token received from the CAS 106 and the token generated from the captured fingerprint information to determine whether the tokens match. See Li at FIG.

3A (step 309) and col. 10, lines 61-64. Hence, Li discloses that the fingerprint capturing device (FCPD) 101 (preferably incorporated into wireless telephone 102) uses the token received from the central authentication system (CAS) 106 in the identification process.

Li discloses that additional security may be provided by having the central authentication system (CAS) 106 also compare the token generated by the user's fingerprint captured and sent by the fingerprint capturing device (FCPD) 101 to one or more stored in the database 107 of the central authentication system (CAS) 106. See Li at FIG. 3B (step 313) and col. 11, lines 10-34 (stating "[t]his second matching of the tokens (note that they were initially compared at step 309) is provided for additional security and may be dispensed with if desired").

As such, Li does not describe or suggest that the checking the read biological information with the stored biological information is carried out by using only the portable communication device, as recited by each of claims 84 and 85. Nor does the rejection's assertion that it would be obvious "that the master user's personal identification number information matched a number stored at the server that the stored biological information could be rewritten" (Action of December 12, 2007 at page 4, line 25 to page 5, line 1) remedy the failure of Li to describe or suggest the subject matter of claims 84 and 85.

Therefore, for at least these reasons, applicant requests reconsideration and withdrawal of the rejection of independent claims 84 and 85.

Claims 1, 26, 51, 54-56, 59-70 and 73-83 have been rejected as being unpatentable over Li in view of U.S. Patent No. 6,839,798 (Nagayoshi), and U.S. Patent No. 6,760,324 (Scott). Applicant requests reconsideration and withdrawal of this rejection because neither Li, Nagayoshi, Scott, nor any proper combination of the references, describes or suggests checking the read biological information with the stored biological information is carried out by using only the checking circuit in the portable communication device, as recited by amended independent claims 1, 26, 51 and 83.

Each of independent claims 1, 26, 51 and 83 is directed to a process or a system in which a portable communication device reads biological information of the client and checks this biological information with reference biological information previously stored in the portable

communication device. Checking the read biological information with the stored biological information is carried out by using only the checking circuit in the portable communication device. Each of independent claims 1, 26, 51 and 83 also recites that, after transmitting information that the checking has matched to the server, a personal identification number information is sent to the server and, in a case that the personal identification number matches with a number stored at the server, the stored biological information can be rewritten.

As described previously with respect to claims 84 and 85, Li does not describe or suggest that checking of the read biological information with the stored biological information is carried out by using only the portable communication device. Hence, Li does not describe or suggest that checking of the read biological information with the stored biological information is carried out by using only the checking circuit in the portable communication device, as recited by amended independent claims 1, 26, 51 and 83.

Nagayoshi is said to disclose a flash memory device which can be used in a mobile phone for storing nonvolatile data. However, Nagayoshi does not describe or suggest that checking of the read biological information with the stored biological information is carried out by using only the checking circuit in the portable communication device, as recited by amended independent claims 1, 26, 51 and 83.

Scott is said to disclose that in a telephone system, a telephone call can be placed from one PSTN to another PSTN over the Internet using Voice over IP and two gateway servers, one on each end of the Internet. Scott, however, does not describe or suggest that checking of the read biological information with the stored biological information is carried out by using only the checking circuit in the portable communication device, as recited by amended independent claims 1, 26, 51 and 83.

Accordingly, neither Li, Nagayoshi, Scott nor any proper combination of the references, describes or suggests that checking of the read biological information with the stored biological information is carried out by using only the checking circuit in the portable communication device, as recited by amended independent claims 1, 26, 51 and 83. Therefore, for at least these reasons, applicant requests reconsideration and withdrawal of the rejection of independent claims

1, 26, 51 and 83, and claims 54-56, 59-70 and 73-82, each of which depends from one of independent claims 1, 26 and 51.

Claims 1, 26, 51, and 54-83 been rejected as being unpatentable over Li in view of Nagayoshi and U.S. Patent No. 5,872,834 (Teitelbaum). Applicant requests reconsideration and withdrawal of this rejection because neither Li, Nagayoshi, Teitelbaum, nor any proper combination of the references, describes or suggests that, after transmitting information that the checking has matched to the server, a personal identification number information is sent to the server and in a case that the personal identification number matches with a number stored at the server, the stored biological information can be rewritten, as recited by amended independent claims 1, 26, 51 and 83.

The rejection concedes that Li fails to specifically disclose that in a case that the personal identification number matches with a number stored at the server the stored biological information can be rewritten. See action of December 12, 2007 at page 4, lines 22-24 (with regard to rejection of claims 84 and 85). The rejection maintains that Li discloses after transmitting information that the checking has matched to the server, a personal identification number information is sent to the server in column 15, paragraphs 3-4 and that Li discloses upon providing the personal identification number information to the server, the stored biological information can be rewritten also in column 15, paragraphs 3-4. See action of December 12, 2007 at page 4, lines 18-22. However, the cited portion of Li describes how a telephone owner could use more than one fingerprint as a means to authenticate his/her identity, how the fingerprint token can be used for billing and authorization purposes, and advantages of using fingerprint tokens. Specifically Li discloses:

> In a further embodiment of the present invention, the phone owner could use more than one fingerprint as a means to authenticate his/her identity. The MCKD 107 can be arranged to contain information regarding more than one fingerprint of the owner. In fact, if additional password-like security beyond fingerprint security is desired, the owner can provide multiple fingerprints from different fingers in a particular secret order. This can serve as a "password" known only to the owner.
>
> In one use of the current invention, the traditional MINs and ESNs associated with wireless phones are no longer required. The wireless telephone 102 will have an integrated FCPD 101. When a user dials a number, the number of the party being called

> and the token generated from the fingerprint of the user on the FCPD 101 will be sent to the MSC 103 and then forwarded to the CAS 106 for authentication based only on the fingerprint token of the user for billing and authorization purposes. Because each fingerprint token generated from the same finger will be different, a token intercepted from the common air interface can not easily be used for fraudulent use of wireless telephones. If a particular token generated from a fingerprint is captured illegally from the air interface and subsequently used repeatedly to authorize illegal calls, this can be detected very easily by the CAS 106 since it would in normal circumstances expect somewhat different and varied tokens being generated from the same fingerprint. Because such variations in the generated token are intrinsic to the way fingerprint information is distributed on the finger itself, these variations cannot be gleaned from illegally capturing one token common from the common air interface. That is, tokens generated from the same fingerprint at different impressions on the FCPD 101 will vary so that merely having illegally captured one of these variations will not enable the generation of varied tokens that are still meaningfully related to the original fingerprint. The only thing that can be done is to use the exact same illegally captured token to make illegal calls, but that can be easily detected. Thus it is possible that the systems of this invention can allow any user to use any wireless telephone to place calls.

Li at col. 15, para. 3-4 (col. 5, line 31 to col. 16, line 3). Li does not disclose in the cited portion sending a personal identification number information to the server, much less that, upon providing the personal identification number information to the server, the stored biological information can be rewritten.

The action asserts that it would have been obvious that "the master user's personal identification number information matches a number stored at the server that the stored biological information could be rewritten ... because the ordinary person skilled in the art would have been motivated to allow an authorized user (a user who's fingerprint matches the master users [sic] fingerprint) to update the biological information." Action of December 12, 2007 at page 4, line 25 to page 5, line 4. As noted previously, Li does not disclose sending a personal identification number information to the server, much less that, upon providing the personal identification number information to the server, the stored biological information can be rewritten.

Therefore, Li does not describe or suggest that, after transmitting information that the checking has matched to the server, a personal identification number information is sent to the server and in a case that the personal identification number matches with a number stored at the

server, the stored biological information can be rewritten, as recited by amended independent claims 1, 26, 51 and 83. The rejection indicates that

Nagayoshi is said to disclose a flash memory device which can be used in a mobile phone for storing nonvolatile data. However, Nagayoshi does not describe or suggest that, after transmitting information that the checking has matched to the server, a personal identification number information is sent to the server and in a case that the personal identification number matches with a number stored at the server, the stored biological information can be rewritten, as recited by amended independent claims 1, 26, 51 and 83.

The rejection asserts that Teitelbaum discloses a telephone storing biometric data of authorized users, captures biometric input from a user, compares the captured biometric information with the stored biometric information, and in the event that there is a match, allowing access to the features of the phone, and in the event that there is not a match, disabling the telephone. See action of December 12, 2007 at page 15, line 21 to page 16, line 4. Even assuming, for the sake of argument only, that the rejection's assertion is correct, such a disclose by Teitelbaum does not remedy Li's failure to describe or suggest after transmitting information that the checking has matched to the server, a personal identification number information is sent to the server and in a case that the personal identification number matches with a number stored at the server, the stored biological information can be rewritten, as recited by independent claims 1, 26, 51 and 83.

Accordingly, Li, Nagayoshi, Teitelbaum, or any proper combination of the references, do not describe or suggest after transmitting information that the checking has matched to the server, a personal identification number information is sent to the server and in a case that the personal identification number matches with a number stored at the server, the stored biological information can be rewritten, as recited by amended independent claims 1, 26, 51 and 83. Therefore, for at least these reasons, applicant requests reconsideration and withdrawal of the rejection of independent claims 1, 26, 51 and 83, and claims 54-82, each of which depends from one of independent claims 1, 26 and 51.

Applicant submits all claims are in condition for allowance.

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

No fee is believed to be due in connection with the filing of this paper on the Electronic Filing System (EFS). In the event that any fees are due, please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: Mar. 11, 2009

Barbara A. Benoit
Reg. No. 54,777

Customer No. 26171
Fish & Richardson P.C
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331